WHAT IS CLAIMED IS:

1. A method of decoding an error-correction code in a data signal, comprising the steps of:

receiving the data signal at a decoding unit;

computing a plurality of syndromes associated with the data signal using the decoding unit;

extracting an error polynomial from the data signal based on no more than six equations having no more than two branch decisions; and

locating errors within the data signal using the error polynomial.

2. The method of Claim 1 wherein said extracting step extracts the error polynomial in no more than 12 clock cycles.

3. The method of Claim 1 wherein said extracting step includes the step of controlling a plurality of Galois field multiply accumulators using a state machine.

4. The method of Claim 3 wherein each of the plurality of Galois field multiply accumulators represents a different power of the error polynomial

5. The method of Claim 1 wherein said computing, extracting, and locating steps use a Bose-Chaudhuri-Hocquenghem (BCH) code.

6. The method of Claim 1 wherein said computing steps computes 2t syndromes, where t is a number of correctable errors which the error-correcting code can correct.

7. The method of Claim 1 wherein said computing step uses a linear feedback register to compute the syndromes.

8. The method of Claim 1 wherein said computing step includes the steps of:

dividing a received code word in the data signal by a minimal Galois polynomial; and

evaluating a remainder from said dividing step.

9. The method of Claim 1 wherein said generating step generates the error polynomial based on the following six equations:

(1) $d_0 = S_1$,

(2) $d_1 = S_3 + S_1 S_2$,

(3) $\sigma^1(x) = 1 + S_1 X$,

(4) if $(d_1 = 0)$ then $\sigma^2(x) = \sigma^1(x)$

else if $(d_0 = 0)$ then $\sigma^2(x) = q_0 \sigma^1(x) + d_1 X^3$

else $\sigma^2(x) = q_0 \sigma^1(x) + d_1 X^2$,

(5) $d_2 = S_5 \sigma_0 + S_4 \sigma_1 + S_3 \sigma_2 + S_2 \sigma_3$, and

(6) if $(d_2 = 0)$ then $\sigma^3(x) = \sigma^2(x)$

else $\sigma^3(x) = q_1 \sigma^1(x) + d_1 X^3$,

where S_i are the syndromes, σ^i are minimum-degree polynomials, σ_i are four coefficients for $\sigma^2(x)$, q_0 is equal to d_0 unless d_0 is zero, when q_0 is 1, and q_1 is equal to d_1 unless d_1 is zero, when $q_1 = q_0$.

10. The method of Claim 1 wherein said generating step includes the step of calculating correction terms using four Galois field multiply accumulators.

11. The method of Claim 1 wherein said locating step locates the errors by determining roots of the error polynomial which correspond to error locations.

12. The method of Claim 11 wherein said locating step uses Chien's algorithm to search for the error location numbers.

13. A method of determining an error polynomial for decoding a Bose-Chaudhuri-Hocquenghem (BCH) code, comprising the steps of:

computing a plurality of syndromes associated with a data signal having a BCH code embedded therein;

feeding the syndromes to a plurality of Galois field multiply accumulators;

calculating a plurality of minimum-degree polynomials associated with the BCH code, using the Galois field multiply accumulators; and

generating an error polynomial based on the minimum-degree polynomials, said calculating and generating steps extracting the error polynomial in no more than 12 clock cycles.

14. The method of Claim 13 wherein said calculating step includes the step of calculating a plurality of coefficients of at least one of the minimum-degree polynomials.

15. The method of Claim 13 wherein said calculating step includes the step of computing a first correction term using at least one of the Galois field multiply accumulators, the first correction term being equal to a first one of the syndromes.

16. The method of Claim 15 wherein said calculating step includes the step of computing a second correction term using at least one of the Galois field multiply accumulators, the second correction term being equal to the sum of a product of the first syndrome with a second one of the syndromes, and a third one of the syndromes

17. The method of Claim 15 wherein said step of computing the first correction term includes the step of operating the at least one Galois field multiply accumulator in a pass-through mode.

18. The method of Claim 13 wherein:

the BCH code is a triple-error correcting code; and

said calculating step calculates at least three minimum-degree polynomials.

19. The method of Claim 18 wherein said calculating step further includes the steps of:

computing a first correction term using at least one of the Galois field multiply accumulators, the first correction term being equal to a first one of the syndromes;

computing a second correction term using at least one of the Galois field multiply accumulators, the second correction term being equal to the sum of a product of the first syndrome with a second one of the syndromes, and a third one of the syndromes; and

computing a third correction term using at least one of the Galois field multiply accumulators, the third correction term being based in part on coefficients of at least one of the minimum-degree polynomials.

20. The method of Claim 19 wherein said calculating step includes the step of determining whether the second correction term is equal to zero.

21. The method of Claim 20 wherein said calculating step equates a first one of the minimum-degree polynomials to a second one of the minimum-degree polynomials in response to a determination that the second correction term is equal to zero.

22. The method of Claim 19 wherein said calculating step includes the step of determining whether the third correction term is equal to zero.

23. The method of Claim 22 wherein said calculating step equates a first one of the minimum-degree polynomials to a second one of the minimum-degree polynomials in response to a determination that the third correction term is equal to zero.

24. The method of Claim 18 wherein there are exactly four of the Galois field multiply accumulators, and said calculating step includes the step of controlling inputs to the Galois field multiply accumulators using a state machine.

25. A circuit for generating an error polynomial of a Bose-Chaudhuri-Hocquenghem (BCH) code, comprising:

a plurality of syndrome inputs;

a plurality of Galois field multiply accumulators; and

means for using said Galois field multiply accumulators to generate an error polynomial based on values provided at said syndrome inputs, by executing no more than six equations with two branch decisions.

26. The circuit of Claim 25 wherein said using means includes a state machine which asserts control ports on the Galois field multiply accumulators to execute the equations.

27. The circuit of Claim 25 wherein said using means computes a first correction term using at least one of the Galois field multiply accumulators, by assigning a value of a first one of the syndromes to the first correction term.

28. The circuit of Claim 27 wherein said using means further computes a second correction term using at least one of the Galois field multiply accumulators, the second correction term being equal to the sum of a product of the first syndrome with a second one of the syndromes, and a third one of the syndromes.

29. The circuit of Claim 27 wherein said using means computes the first correction term by operating at least one Galois field multiply accumulator in a pass-through mode.

30. The circuit of Claim 25 wherein said using means uses the Galois field multiply accumulators to calculate a plurality of minimum-degree polynomials associated with the BCH code.

31. The circuit of Claim 30 wherein said using means uses the Galois field multiply accumulators to calculate a plurality of coefficients of at least one of the minimum-degree polynomials.

32. The circuit of Claim 30 wherein:

the BCH code is a triple-error correcting code; and

said using means uses the Galois field multiply accumulators to calculate at least three minimum-degree polynomials.

33. The circuit of Claim 30 wherein said using means uses the Galois field multiply accumulators to:

compute a first correction term, by assigning a value of a first one of the syndromes to the first correction term;

compute a second correction term, the second correction term being equal to the sum of a product of the first syndrome with a second one of the syndromes, and a third one of the syndromes; and

compute a third correction term, the third correction term being based in part on coefficients of at least one of the minimum-degree polynomials.

34. The circuit of Claim 33 wherein said using means includes means for determining whether the second correction term is equal to zero.

35. The circuit of Claim 34 wherein said using means equates a first one of the minimum-degree polynomials to a second one of the minimum-degree polynomials in response to a determination that the second correction term is equal to zero.

36. The circuit of Claim 33 wherein said using means includes means for determining whether the third correction term is equal to zero.

37. The circuit of Claim 36 wherein said using means equates a first one of the minimum-degree polynomials to a second one of the minimum-degree polynomials in response to a determination that the third correction term is equal to zero.

38. A decoder circuit comprising:

a plurality of Galois field multiply accumulators; and

a state machine programmed to use said Galois field multiply accumulators to generate an error polynomial based on the following six equations:

(1) $d_0 = S_1$,

(2) $d_1 = S_3 + S_1 S_2$,

(3) $\sigma^1(x) = 1 + S_1 X$,

(4) if $(d_1 = 0)$ then $\sigma^2(x) = \sigma^1(x)$

else if $(d_0 = 0)$ then $\sigma^2(x) = q_0\sigma^1(x) + d_1X^3$

else $\sigma^2(x) = q_0\sigma^1(x) + d_1X^2$,

(5) $d_2 = S_5\sigma_0 + S_4\sigma_1 + S_3\sigma_2 + S_2\sigma_3$, and

(6) if $(d_2 = 0)$ then $\sigma^3(x) = \sigma^2(x)$

else $\sigma^3(x) = q_1\sigma^1(x) + d_1X^3$,

where S_i are error syndromes, σ^i are minimum-degree polynomials, σ_i are four coefficients for $\sigma^2(x)$, q_0 is equal to d_0 unless d_0 is zero, when q_0 is 1, and q_1 is equal to d_1 unless d_1 is zero, when $q_1 = q_0$.

39. The decoder circuit of Claim 38 wherein each of the Galois field multiply accumulators represents a different power of the error polynomial.

40. The decoder circuit of Claim 38 wherein said state machine is programmed to operate a selected one or more of said Galois field multiply accumulators in a pass-through mode.

41. The decoder circuit of Claim 38 wherein said state machine and said Galois field multiply accumulators are formed in a common application-specific integrated circuit.

42. The decoder circuit of Claim 38 wherein:

the BCH code is a triple-error correcting code; and

there are exactly four of said Galois field multiply accumulators.

43. The decoder circuit of Claim 42 wherein equation (1) is performed using a first one of said Galois field multiply accumulators.

44. The decoder circuit of Claim 43 wherein equation (2) is performed using said first Galois field multiply accumulator and a second one of said Galois field multiply accumulators.

45. The decoder circuit of Claim 44 wherein equation (3) is performed using said first and second Galois field multiply accumulators.

46. The decoder circuit of Claim 38 wherein:

at least one of said Galois field multiply accumulators has a first multiplexer whose output is coupled to a first input of a Galois field multiplier, a second multiplexer whose output is coupled to a second input of said Galois field multiplier, and a third multiplexer whose output is coupled to a first input of a Galois field adder, wherein an output of said Galois field multiplier is further coupled to a second input of said Galois field adder; and

said state machine controls respective select lines for each of said multiplexers.

47. The decoder circuit of Claim 46 further comprising means for determining when an output of said Galois field adder is equal to zero.

48. An OC-192 input/output card comprising:

four OC-48 processors; and

an OC-192 front-end application-specific integrated circuit (ASIC) connected to said four OC-48 processors, said OC-192 front-end ASIC having means for de-interleaving an OC-192 signal to create four OC-48 signals, and means for decoding error-correction codes embedded in each of the four OC-48 signals, said decoding means including means for generating an error polynomial associated with a given one of the error-correction codes in no more than 12 clock cycles.

49. The OC-192 input/output card of Claim 48 wherein said decoding means includes a plurality of Galois field multiply accumulators.

50. The OC-192 input/output card of Claim 49 wherein said decoding means further includes a state machine controlling said Galois field multiply accumulators.

51. The OC-192 input/output card of Claim 49 wherein said decoding means uses said Galois field multiply accumulators to generate an error polynomial for a Bose-Chaudhuri-Hocquenghem (BCH) triple-error correcting code.

52. The OC-192 input/output card of Claim 51 wherein said decoding means includes no more than four of said Galois field multiply accumulators.

53. The OC-192 input/output card of Claim 51 wherein said decoding means includes means for computing a plurality of BCH syndromes which are used by said Galois field multiply accumulators to generate the error polynomial.

54. The OC-192 input/output card of Claim 48 wherein said decoding means locates errors within the data signal by applying Chien's algorithm to the error polynomial to search for error location numbers.